**Traccia: Tecniche di scansione con Nmap**

Si richiede allo studente di effettuare le seguenti scansioni sul target **Metasploitable**:

- OS fingerprint
- Syn Scan
- TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?
- Version detection

Modificate le impostazioni di rete delle macchine virtuali per fare in modo che i due target siano sulla stessa rete. A valle delle scansioni, per entrambi gli IP, è prevista la produzione di un **report** contenente le seguenti info (dove disponibili):

- IP
- Sistema Operativo
- Porte Aperte
- Servizi in ascolto con versione
- Descrizione dei servizi

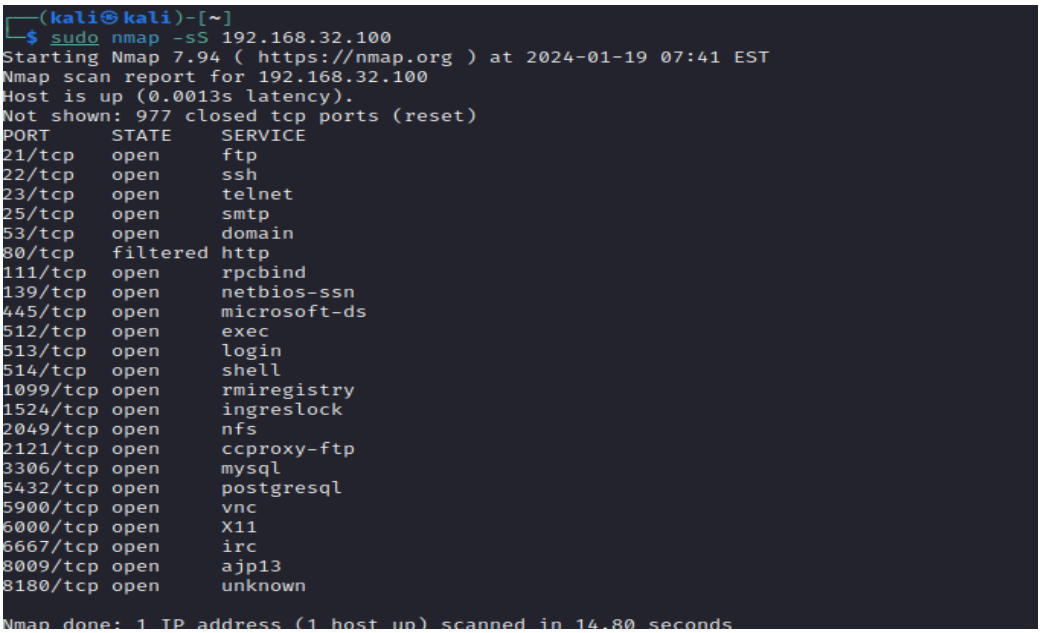
https://www.poftut.com/nmap-output/

nmap -oN report1 IP

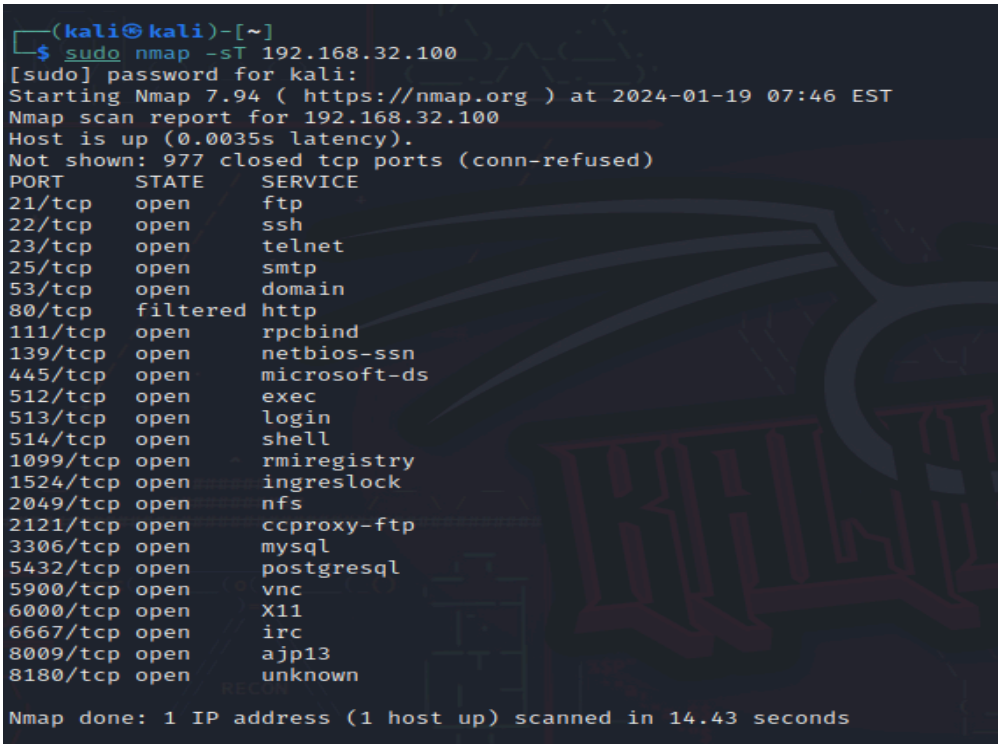
## 1. OS FINGERPRINT

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.32.100
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 07:39 EST
Nmap scan report for 192.168.32.100
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   filtered http
111/tcp  open     rpcbind
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
512/tcp  open     exec
513/tcp  open     login
514/tcp  open     shell
1099/tcp open     rmiregistry
1524/tcp open     ingreslock
2049/tcp open     nfs
2121/tcp open     ccproxy-ftp
3306/tcp open     mysql
5432/tcp open     postgresql
5900/tcp open     vnc
6000/tcp open     X11
6667/tcp open     irc
8009/tcp open     ajp13
8180/tcp open     unknown
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded), Linux 2.6.20 - 2.6.24 (Ubuntu 7.04 - 8.04)
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.32 seconds

┌──(kali㉿kali)-[~]
└─$
```

2. Syn Scan

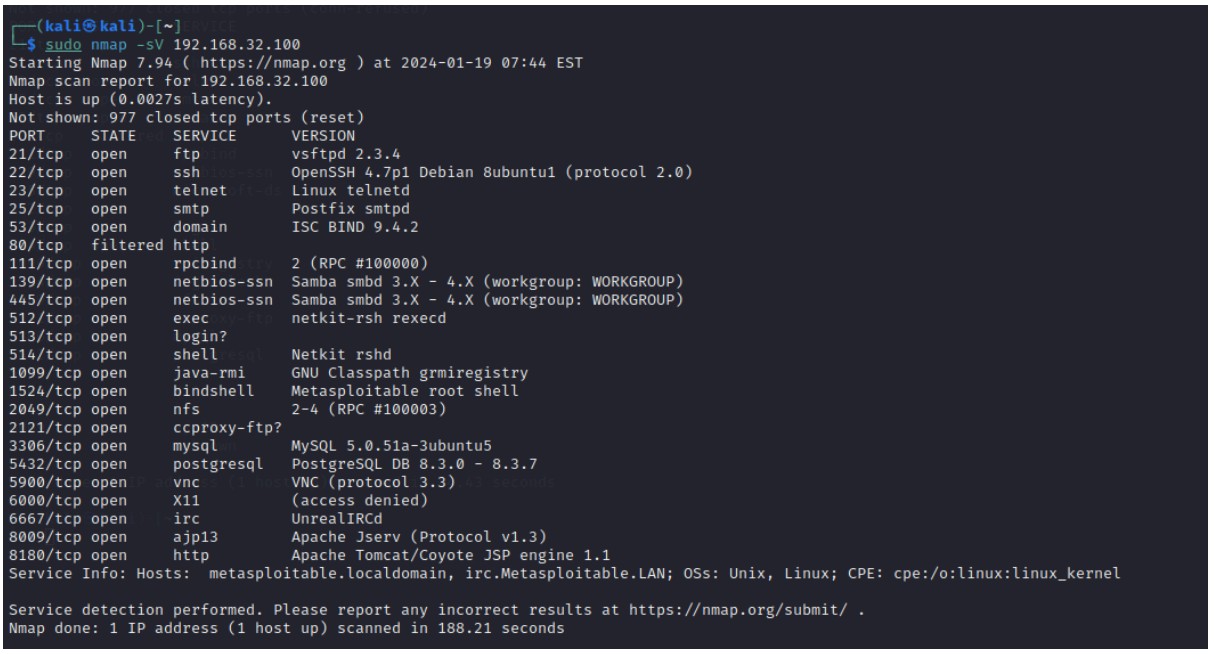



3. TCP scan




Tra in 3 tipi di scansione non si rilevano differenze sostanziali.

4. sV scan



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.32.100
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 07:44 EST
Nmap scan report for 192.168.32.100
Host is up (0.0027s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE    SERVICE      VERSION
21/tcp   open     ftp          vsftpd 2.3.4
22/tcp   open     ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open     telnet       Linux telnetd
25/tcp   open     smtp         Postfix smtpd
53/tcp   open     domain       ISC BIND 9.4.2
80/tcp   filtered http
111/tcp  open     rpcbind      2 (RPC #100000)
139/tcp  open     netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open     netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open     exec         netkit-rsh rexecd
513/tcp  open     login?
514/tcp  open     shell        Netkit rshd
1099/tcp open     java-rmi     GNU Classpath grmiregistry
1524/tcp open     bindshell    Metasploitable root shell
2049/tcp open     nfs          2-4 (RPC #100003)
2121/tcp open     ccproxy-ftp?
3306/tcp open     mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp open     postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open     vnc          VNC (protocol 3.3)
6000/tcp open     X11          (access denied)
6667/tcp open     irc          UnrealIRCd
8009/tcp open     ajp13        Apache Jserv (Protocol v1.3)
8180/tcp open     http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 188.21 seconds
```

Per l’esportazione del report preferisco utilizzare la scansione sV in quanto fornisce anche informazioni di massima sul sistema.

```
└─$ sudo nmap -sV -oN report1.txt -v 192.168.32.100
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 07:53 EST
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 07:53
Scanning 192.168.32.100 [4 ports]
Completed Ping Scan at 07:53, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:53
Completed Parallel DNS resolution of 1 host. at 07:53, 13.03s elapsed
Initiating SYN Stealth Scan at 07:53
Scanning 192.168.32.100 [1000 ports]
Discovered open port 5900/tcp on 192.168.32.100
Discovered open port 25/tcp on 192.168.32.100
Discovered open port 139/tcp on 192.168.32.100
Discovered open port 3306/tcp on 192.168.32.100
Discovered open port 445/tcp on 192.168.32.100
Discovered open port 21/tcp on 192.168.32.100
Discovered open port 53/tcp on 192.168.32.100
Discovered open port 22/tcp on 192.168.32.100
Discovered open port 111/tcp on 192.168.32.100
Discovered open port 23/tcp on 192.168.32.100
Discovered open port 512/tcp on 192.168.32.100
Discovered open port 8009/tcp on 192.168.32.100
Discovered open port 6667/tcp on 192.168.32.100
Discovered open port 6000/tcp on 192.168.32.100
Discovered open port 1099/tcp on 192.168.32.100
Discovered open port 2121/tcp on 192.168.32.100
Discovered open port 5432/tcp on 192.168.32.100
Discovered open port 8180/tcp on 192.168.32.100
Discovered open port 513/tcp on 192.168.32.100
Discovered open port 514/tcp on 192.168.32.100
Discovered open port 1524/tcp on 192.168.32.100
Discovered open port 2049/tcp on 192.168.32.100
Completed SYN Stealth Scan at 07:53, 1.26s elapsed (1000 total ports)
Initiating Service scan at 07:53
Scanning 22 services on 192.168.32.100
Completed Service scan at 07:56, 157.12s elapsed (22 services on 1 host)
NSE: Script scanning 192.168.32.100.
Initiating NSE at 07:56
Completed NSE at 07:56, 8.14s elapsed
Initiating NSE at 07:56
Completed NSE at 07:56, 8.05s elapsed
Nmap scan report for 192.168.32.100
Host is up (0.0019s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE    SERVICE      VERSION
21/tcp   open     ftp          vsftpd 2.3.4
22/tcp   open     ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
```

```
└─$ cat report1.txt
# Nmap 7.94 scan initiated Fri Jan 19 07:53:25 2024 as: nmap -sV -oN report1.txt -v 192.168.32.100
Nmap scan report for 192.168.32.100
Host is up (0.0019s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE    SERVICE      VERSION
21/tcp   open     ftp          vsftpd 2.3.4
22/tcp   open     ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open     telnet       Linux telnetd
25/tcp   open     smtp         Postfix smtpd
53/tcp   open     domain       ISC BIND 9.4.2
80/tcp   filtered http
111/tcp  open     rpcbind      2 (RPC #100000)
139/tcp  open     netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open     netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open     exec         netkit-rsh rexecd
513/tcp  open     login?
514/tcp  open     shell        Netkit rshd
1099/tcp open     java-rmi     GNU Classpath grmiregistry
1524/tcp open     bindshell    Metasploitable root shell
2049/tcp open     nfs          2-4 (RPC #100003)
2121/tcp open     ccproxy-ftp?
3306/tcp open     mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp open     postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open     vnc          VNC (protocol 3.3)
6000/tcp open     X11          (access denied)
6667/tcp open     irc          UnrealIRCd
8009/tcp open     ajp13        Apache Jserv (Protocol v1.3)
8180/tcp open     http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Jan 19 07:56:33 2024 -- 1 IP address (1 host up) scanned in 188.10 seconds
```